



DECEPTION TECHNOLOGY
BY



CYBERTRAP



ANGRIFFE
**ERKENNEN,
ÜBERWACHEN UND
KONTROLLIEREN**



DATEN
**SICHERN,
SCHÜTZEN UND
KONTROLLIEREN**



Authentische Angriffsziele
für Angreifer



Auf Ihre Infrastruktur
maßgeschneidert



Nicht erkennbar
für Angreifer



Enthält keine für Angreifer
verwertbaren Informationen



CyberTrap versteht die täglichen Herausforderungen der Angriffsprävention und bietet signifikante Unterstützung mittels revolutionärer Technologie, zielgerichtete Angriffe in Echtzeit zu erkennen und Angreifer sowie deren Absichten zu identifizieren.

CyberTrap überwindet die Grenzen der Prävention

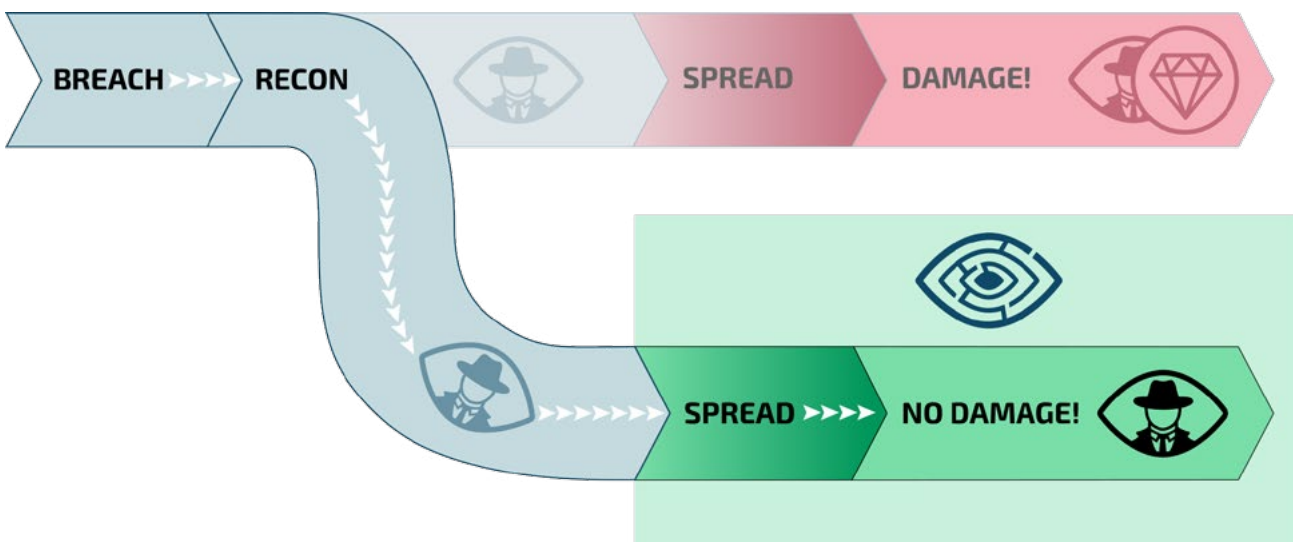
In modernen Netzwerken haben es präventive Maßnahmen schwer die IT-Infrastruktur abzusichern. Neue Angriffsszenarien umgehen die bestehenden Abwehrmaßnahmen. Digitale Geschäftsprozesse erfordern daher zusätzliche Sicherheitskonzepte.

Eine zunehmend komplexere IT Infrastruktur ist zur Lebensader eines jeden modernen Unternehmens geworden. Eine wachsende Anzahl interner wie externer Anwendungen und Anwender tragen maßgeblich zu dieser Entwicklung bei und erhöhen die Komplexität auf ein Niveau, dass sich nur noch schwer absichern lässt. Angreifer adaptieren ihre Angriffsmethoden und stellen präventive Sicherheitsmaßnahmen vor überwältigende Herausforderungen. Als Konsequenz schaffen es Sicherheitssysteme heute nicht mehr Netzwerke zuverlässig vor Angreifern zu schützen. Es ist fast so, als würde man versuchen einen endlosen Zaun Loch für Loch zu flicken - es ist teuer und niemals schnell genug.

CyberTrap ist die Lösung

CyberTrap agiert hinter der Firewall und dient als Fangnetz für Angreifer, welche die bestehenden Sicherheitssysteme überwinden.

CyberTrap ist ein revolutionärer neuer Ansatz in der IT-Sicherheit. Anstatt vergeblich zu versuchen Angreifer auszusperrern, werden sie aus dem internen Netzwerk in eine geschlossene, überwachte Umgebung umgeleitet, um sie dort zu beobachten und Informationen über sie zu sammeln. Damit zeigt uns der Angreifer nicht nur die Löcher im Zaun, sondern verrät uns auch, wer er ist und wonach er sucht.



Mit anderen Worten: CyberTrap ist mehr als nur ein Honeypot – CyberTrap ist eine überwachte Umgebung:

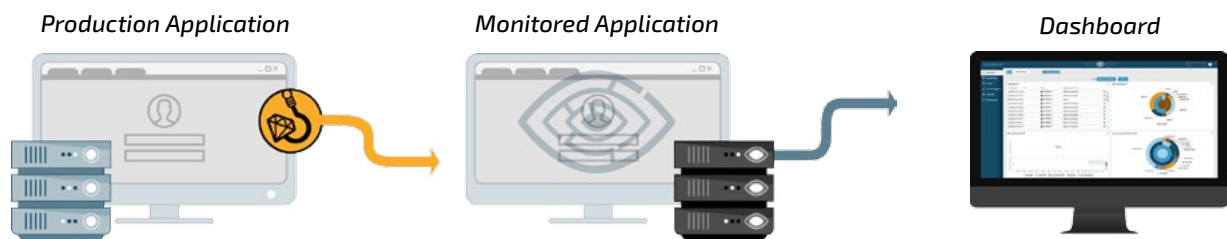
- Wirkt auf Angreifer absolut authentisch
- Für Ihre Infrastruktur maßgeschneidert
- Verwendung von echten Betriebssystemen und Diensten
- Enthält keine für Angreifer verwertbaren Informationen
- Nicht erkennbar für Angreifer

Technische Übersicht

CyberTrap bietet Ihnen unterschiedliche Möglichkeiten um eine maßgeschneidert Deception-Umgebung zu schaffen. Es wird dabei viel Wert auf einfache Handhabung gelegt, um die hohe technische Komplexität und die Vielfalt an Funktionen im Alltag nutzbar zu machen.

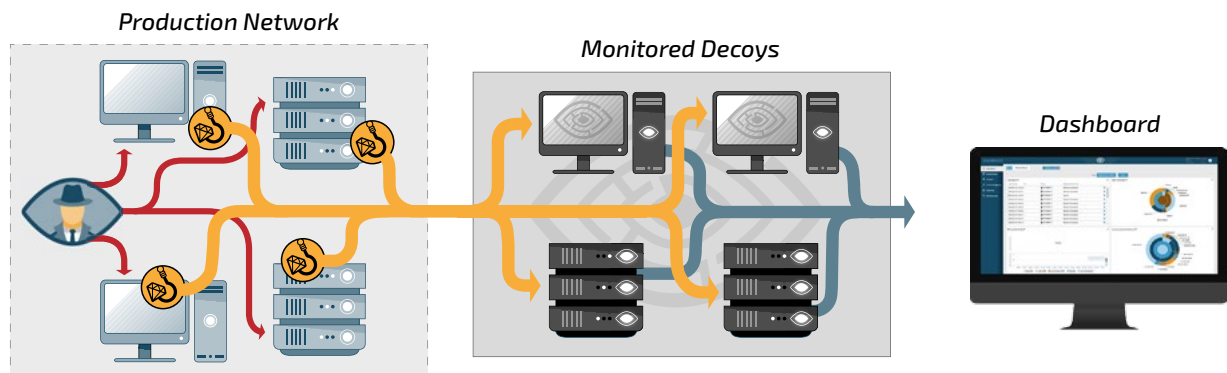
WEB-APPLIKATION-DECEPTION

Wir hinterlegen Köder an strategisch wichtigen Positionen im Kontext Ihrer produktiven Webanwendungen. Bei Ködern handelt es sich nicht um Software, sondern um Konfigurationen und Dateien. Diese Köder sind für den normalen Besucher nicht sichtbar, werden jedoch bei zielgerichteten Angriffen gefunden. Die Köder sind mit speziell erstellten Fallen verbunden. Sobald der Angreifer in eine dieser Fallen gelenkt wurde, wird sein Verhalten überwacht und jede seiner Bewegungen beobachtet.



ENDPOINT-DECEPTION

Die Köder werden auf produktiven Endgeräten hinterlegt wo sie bei legitimer Nutzung nicht erkennbar sind. Der Angreifer wird jedoch bei der Suche nach wertvollen Informationen und Daten auf die Köder stoßen, welche ihn in die Fallen leiten. Für den Angreifer ist kein Unterschied zwischen der realen Umgebung und den Fallen erkennbar, da sie auf das reale Netzwerk zugeschnitten sind. Zudem werden sie mit Daten gefüllt, die für den Angreifer authentisch aussehen, aber keine wertvollen Informationen beinhalten.



INDIVIDUELL ABGESTIMMTE UMGEBUNGEN

Das Täuschen eines Angreifers hat zwei Ebenen: Eine technische und eine psychologische.


Auf der technischen Ebene ist vieles möglich. Köder können beispielsweise versteckte Dateifreigaben sein, die nur vom Angreifer gesehen werden können, oder gespeicherte Anmeldeinformationen, die ihn in unsere Fallen locken.

Die psychologische Ebene ist komplexer. Es ist wichtig, die Produktionsumgebung genau zu betrachten und die Deception-Umgebung automatisiert auf den jeweiligen Kontext zuzuschneiden.

TRACKDOWN


TrackDown-Dokumente sind mit digitalen Peilsendern versehen, die beim Entwerden aus der CyberTrap Umgebung eine Verbindung aufbauen. Es werden dadurch detaillierte Informationen über den Angreifer einsehbar. Die Technologie funktioniert mit verschiedenen Formaten und Anwendungen.

TrackDown lässt sich nahtlos mit dem Full Stack-Deception-Konzept integrieren, da markierte Dokumente strategisch in Fallen platziert werden können.



Supported Service

- Regelmäßige Updates
- Hotline-Support
- Schulung für das Cybertrap Dashboard

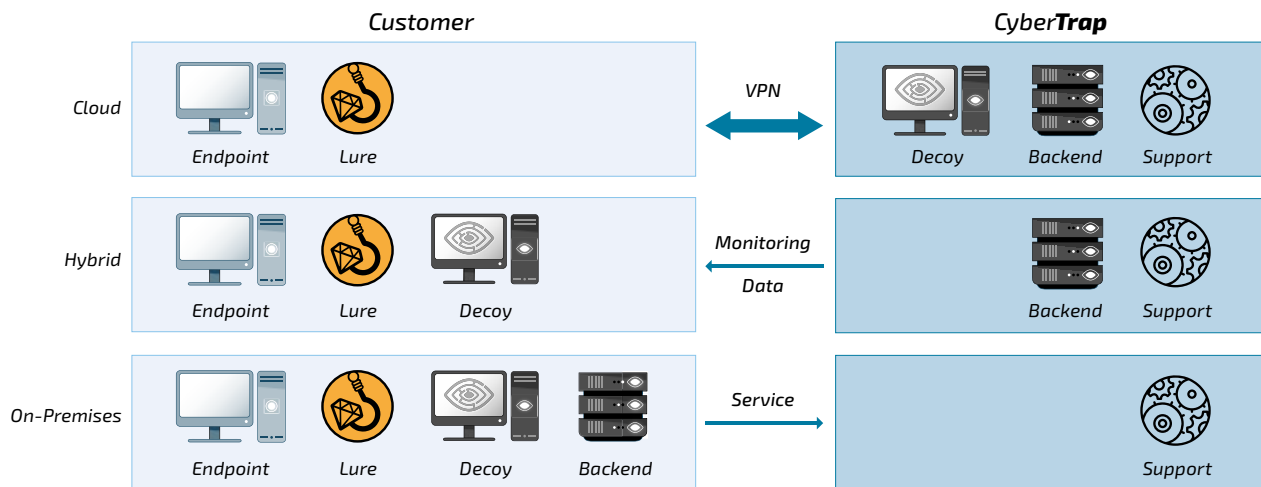


Managed Service

- Regelmäßige Updates
- Hotline-Support
- Schulung für das Cybertrap Dashboard
- Schnellanalyse bei Vorfällen
- Monatlicher Bericht
- Unterstützung durch Experten bei Angriffen

Implementierungsoptionen

CyberTrap lässt sich auf drei verschiedene Arten implementieren: Cloud, On-Premise oder Hybrid.



Das Unternehmen

CyberTrap ist ein Cybersicherheitsunternehmen mit Sitz in Wien, Österreich, das sich auf Deception Technologie für Behörden und Großunternehmen in Europa spezialisiert hat. Das Unternehmen wurde 2015 als Resultat eines erfolgreichen Kunden-Projekts von SEC Consult, einem führenden europäischen Beratungsunternehmen für Cybersicherheit, gegründet. Nach mehrjähriger interner Weiterentwicklung führte CyberTrap seine bahnbrechende Deception as a Service Technologie im Jahre 2017 in den Markt ein. CyberTrap will den Zugang zu fortschrittlicher Deception Technologie damit auch für mittelständische Unternehmen ermöglichen.